Sense of Security™
Security that enables business

Achieving PCI Compliance: Long and Short Term Strategies

Murray Goldschmidt - CISSP, QSA

PCI DSS Compliance Conference, 3 Dec 2009

Overview

1. PCI Compliance - A Business or IT Issue?
2. The Key Elements of a Successful PCI DSS Compliance Assessment
3. Building a Roadmap to PCI DSS Compliance
4. Long and Short Term Strategies
5. Conclusion

Why is PCI DSS Seen as an IT Issue?

Take a good look at the wording of the 12 core requirements:

PCI DSS Requirements

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Sense of Security™
Security that enables business

Why is PCI DSS Seen as an IT Issue?

- Organisations often do not look beyond the 12 requirements before assigning PCI DSS compliance responsibilities
- Therefore PCI DSS becomes an IT “project”
- PCI DSS contains ~270 sub-requirements

Sense of Security™
Security that enables business

PCI DSS is a Business Issue

- PCI DSS is not a project and should not be treated as one
  - PCI DSS has no start or finish date
  - As with security in general, PCI DSS is an ongoing process
  - IT is a project based culture
- PCI DSS addresses business risk, not IT risk
  - It requires people that understand the business and can align PCI DSS requirements with business risk
  - PCI DSS should be addressed at the business level via an organisation's overall compliance framework
- Cost of compliance sits with the business
  - Cost does not sit with an individual department
  - The risk to business and cost of non-compliance far exceed the implementation costs
  - Data compromise affects the entire organisation

Sense of Security™
Security that enables business

Key Elements of a Successful Audit

- PCI DSS is about policy, process and procedures
  - Technology provides the tools to help achieve the goal
  - PCI DSS is about more than just technical issues or finding technical solutions
- Do not pass responsibility to the IT department
  - The scope and size of a PCI DSS audit is too much for one department
  - Spans other areas not under IT control
- Obtain backing from the business
  - The lead for driving compliance must reside on the business side
  - Requires support from those that understand the business
  - The business must remain involved throughout the life of PCI DSS
  - Resources span departments and requires authority to assign these resources

Sense of Security™
Security that enables business

Key Elements of a Successful Audit

- Reduce your scope
- Prioritise
- PCI DSS requirements should not be addressed in isolation
  - Individual IT solutions create complex and unmanageable environments
  - There is no silver bullet
  - Manageability issues lead to security issues
- Choose the right QSA
  - PCI DSS spans a vast number of disciplines
  - The QSA should have in-depth knowledge and experience in all areas
- Remember: PCI DSS compliance is a snapshot of an organisation's compliance at a single point in time
  - Compliance != Security
  - Ongoing adherence to process and procedures should ensure ongoing compliance

Sense of Security™
Security that enables business

Roadmap to Compliance - Short Term

- PCI DSS is based on security best practice
- Prioritise
  - PCI DSS is a set of guidelines to reduce risk
  - Not all requirements are equal in size or complexity
  - PCI DSS Prioritised Approach
- Reduce your scope, reduce your data
  - Where is the risk if there is nothing to steal?
  - Outsourcing: Why and why not
- Protect your networks
  - Perimeter
  - Internal
  - Wireless
- Lock and secure the front door
  - Payment applications access sensitive data

Sense of Security™
Security that enables business

Roadmap to Compliance - Long Term

- Monitor and control access
  - Who is accessing your data?
- Protect stored data
  - How will you protect your data?
  - Stored and in transit
- Ongoing policies, processes and procedures
  - PCI DSS is a process, not a project
  - If policy, process and procedures are followed, compliance can be maintained

Conclusion

- PCI DSS addresses business risk and cannot be solved piecemeal with IT solutions
- PCI DSS not a project, it is about policy and processes
- Get backing from the business from day one
- Reduce your scope
- Prioritise
- By applying good security practice and following established policy and procedures, the organisation can obtain not only PCI DSS compliance but also overall security

Thank You

Questions?

Murray Goldschmidt
Sense of Security Pty Ltd
murrayg@senseofsecurity.com.au
Tel: +61 2 9290 4444
http://www.senseofsecurity.com.au